

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-185006

(43)Date of publication of application : 09.07.1999

(51)Int.Cl.

G06K 19/10

G06K 17/00

G06K 19/07

(21)Application number : 09-357103

(71)Applicant : DAINIPPON PRINTING CO LTD

(22)Date of filing : 25.12.1997

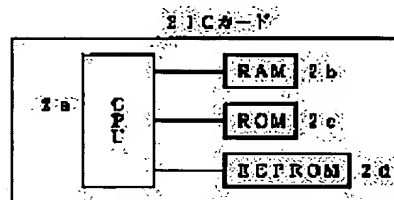
(72)Inventor : HAYASHI MASAHIRO

(54) IC CARD

(57)Abstract:

PROBLEM TO BE SOLVED: To prevent illegal access from the outside of a card and to improve security without increasing the kind of dedicated file by arranging a flag for specifying the ability/disability of execution for every operation in each data area.

SOLUTION: An IC card 2 has a CPU 2a and an EEPROM 2d as a non-volatile memos. The mutual certification is performed between terminal equipment and the IC card 2 and after the certification is established, read/write into memories 2a-2d of the IC card 2 is possible. Concerning the EEPROM 2d, the flags (addition flag, subtraction flag, multiplication flag and division flag) for specifying the ability/disability of execution for every operation are arranged in data areas. The set/cancel of the flag is certified by password collection, password certification and fingerprint or the like. In the case of addition to be used for the accumulation of how many times the card is utilized, while referring to the flag set in an addition data file, addition is performed by an adding instruction when the flag is turned on.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of

rejection]

[Date of requesting appeal against examiner's
decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2000 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平 1 1 - 1 8 5 0 0 6

(43) 公開日 平成 1 1 年 (1 9 9 9) 7 月 9 日

(51) Int. Cl.

識別記号

庁内整理番号

F I

技術表示箇所

G06K 19/10

G06K 19/00

R

17/00

17/00

T

19/07

19/00

N

審査請求 未請求 請求項の数 2 O L (全 5 頁)

(21) 出願番号 特願平 9 - 3 5 7 1 0 3

(22) 出願日 平成 9 年 (1 9 9 7) 1 2 月 2 5 日

(71) 出願人 0 0 0 0 0 2 8 9 7

大日本印刷株式会社

東京都新宿区市谷加賀町一丁目 1 番 1 号

(72) 発明者 林 昌弘

東京都新宿区市ケ谷加賀町一丁目 1 番 1 号

大日本印刷株式会社内

(74) 代理人 弁理士 蛭川 昌信 (外 7 名)

(54) 【発明の名称】 I C カード

(57) 【要約】

【課題】 専用のファイルの種類を増やすことなく、カード外からの不正なアクセスを防止してセキュリティを向上させる。

【解決手段】 端末装置と I C カード間で相互に認証し、認証成立後 I C カードのメモリの読み書きを可能とし、不揮発性メモリのデータエリアでの演算機能を有する I C カードにおいて、演算ごとに実行可／不可を規定するフラグを各データエリアに配し、フラグの状態によって演算命令を制御することを特徴とする。

E E P R O M

加算 E F	減算 E F	乗算 E F	除算 E F
フラグ	フラグ	フラグ	フラグ

【特許請求の範囲】

【請求項 1】 制御手段、RAM、不揮発性メモリ、ROMを有し、端末装置とICカード間で相互に認証し、認証成立後ICカードのメモリの読み書きを可能とし、不揮発性メモリのデータエリアでの演算機能を有するICカードにおいて、演算ごとに実行可／不可を規定するフラグを各データエリアに配したことを特徴とするICカード。

【請求項 2】 請求項 1 記載のICカードにおいて、前記フラグはデータエリアの管理者権限を有する認証によって解除、設定が可能であることを特徴とするICカード。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、不揮発性メモリとして、例えば、EEPROM (Electrically Erasable and Programmable Read Only Memory) を有し、カード内のデータエリアでの演算機能を有する制御機能付きICカードに関する。

【0002】

【従来の技術】近年、プリペイドカード等さまざまな形で使用されているICカードは、図4に示すように、リーダ／ライタ1とICカード2間で互いに認証し、相手が真正であると判断した場合にICカードのメモリの読み書きを可能としている。その場合、演算はリーダ／ライタ1で実施し、結果をICカード内部へ転記する方式や、図4に示すように、リーダ／ライタ1からICカード2に対してコマンドを送信し、これを受信したICカードは、コマンドを解釈して書き込み／読み出し等の処理を実行し、処理結果をレスポンスとしてリーダ／ライタ1へ返す方式がある。

【0003】図5に示すように、ICカード2は、制御手段としてのCPU2a、RAM2b、ROM2c、不揮発性メモリとしてのEEPROM2dを有しており、ROM2cに記憶されているプログラムをCPU2aに読み込み、リーダ／ライタ1から送信されるコマンドをI/Oポートを通して受信すると、コマンドとともに送信されたデータを読み込んで必要な処理を行い、結果をEEPROM2dの所定のファイルに書き込み、I/Oポートを通してレスポンスを出力する。

【0004】認証処理は、リーダ／ライタとICカード側で同じ照合用のデータ(パスワード)をもっておき、これらと比較することにより行う。例えば、ICカード側における認証について説明すると、図6(a)に示すように、リーダ／ライタ1から送られてきたデータ長Lの照合コマンドと、図6(b)に示すような、ICカード自身が持っている長さL'の照合データとを比較する。

【0005】図7に示すように、まずデータ長LとL'とを比較し、L≠L'であれば照合NGであり、リーダ

／ライタ1は真正なものではないと判断される。L=L'であれば、データ内容について照合し、内容が一致すれば照合OKとなり、リーダ／ライタ1は真正なものであると判断される。

【0006】また、パスワードに代えて、乱数を発生させて暗号を生成し、これを用いて相互に認証することも行われている。

【0007】

【発明が解決しようとする課題】従来のCPU付きICカードは、コマンド制御をパスワード照合、あるいは暗号認証で制御していたため、パスワードや暗号が盗用されたとき、ICカード内のデータの書き換えが自由に行われてしまう。

【0008】本発明は上記課題を解決するためのもので、専用のファイルの種類を増やすことなく、カード外からの不正なアクセスを防止してセキュリティを向上させることを目的とする。

【0009】

【課題を解決するための手段】本発明は、制御手段、RAM、不揮発性メモリ、ROMを有し、端末装置とICカード間で相互に認証し、認証成立後ICカードのメモリの読み書きを可能とし、不揮発性メモリのデータエリアでの演算機能を有するICカードにおいて、演算ごとに実行可／不可を規定するフラグを各データエリアに配したことを特徴とする。また、本発明は、フラグはデータエリアの管理者権限を有する認証によって解除、設定が可能であることを特徴とする。

【0010】

【発明の実施の形態】以下、本発明のICカードの実施の形態について説明する。なお、本発明のICカードの構成は図4、図5で示したような制御手段としてのCPU、RAM、不揮発性メモリとしてEEPROM、ROMを有し、端末装置とICカード間で相互に認証し、認証成立後ICカードのメモリの読み書きを可能とするものであり、制御手段としてはCPU以外にもワイヤードロジック等も含み、不揮発性メモリとしてはEEPROM以外にもFRAM(強誘電体性メモリ)等も含むものである。図1は不揮発性メモリをEEPROMとしたときのメモリ内のファイルを説明する図、図2は購買可能金額の設定処理フローを説明する図、図3は減算処理フローを説明する図である。図1は四則演算の場合に、演算ごとに実行可能／実行不可能を規定するフラグ(加算フラグ、減算フラグ、乗算フラグ、減算フラグ)をデータエリアに配してフラグにより演算命令を制御する例を示している。このフラグは、データの桁あふれ、基準値に満たない等のため演算が実行できない場合や、特定の演算のみ実行可能にして、他の演算は実行不可にする場合等に用いる。このフラグの設定、解除は、データエリアの管理者権限を持つ認証の成功を必要とする。この場合の認証例としては、パスワード照合、暗号認証、指紋

等の生体認証があり、これらの1つ、或いは複数を組み合わせて用いる。

【0011】図1に示すデータエリアにアクセスするためには、まず、パスワード照合、あるいは暗号認証によってアクセス権を得ることが必要である。アクセス権を得た後、演算が可能となるのは、演算フラグがONになっている場合である。例えば、カードの利用回数の積算等に用いられる加算では、加算データファイル(EF)に設定されているフラグを参照し、フラグがONの場合に加算処理が実行可能となり、加算命令により加算が行われる。なお、EFはデータ等を格納する基礎ファイルを意味している。例えば、プリペイドカードで使用した料金の減額等に利用される減算では、減算データファイル(EF)のフラグを参照し、フラグがONの場合に減算処理が実行可能となり、減算命令により減算が行われる。例えば、使用度数と1度数当たりの費用との積を演算する場合等に用いられる乗算では、乗算データファイル(EF)のフラグを参照し、フラグがONの場合に乗算処理が実行可能となり、乗算命令により乗算が行われる。例えば、残額を1度数当たりの費用で除算して残り利用可能回数を演算する場合等に用いられる除算では、除算データファイル(EF)のフラグを参照し、フラグがONの場合には除算処理が実行可能となり、除算命令により除算が行われる。

【0012】そして、これらの演算において所定のフラグがOFFの場合には、その演算は禁止され、リーダ/ライタ側から演算命令を出してもそのエリアの演算は実行されず、このことは、例えば、リーダ/ライタを通して表示等の手段により通知される。なお、上記では四則演算を対象にして説明したが、本発明はこれに限らず、データエリアで行われる任意の演算に対してフラグを配し、各エリアに適用される演算命令を制御することも可能である。

【0013】次に、本発明のICカードをプリペイド用途に利用する場合を例にとって以下に説明する。図2は購買可能金額設定処理フローを示す図である。まず、プリペイドカードのチャージ(加算)用認証を実施する(S1)。この認証は、データエリアの管理者権限を持つ認証である。プリペイド金額の加算条件として、例えば、パスワード照合、暗号認証、指紋等の生体認証等の認証を利用する。認証が成功しない場合には(S2 NO)、処理は行われず、認証の成功により(S2 YES)、加算フラグ、減算フラグをONにし(S3)、加算処理してプリペイド領域に購買可能金額を設定する(S4)。次いで、購買可能金額の改ざん防止のために加算フラグをOFFにして加算禁止にする(S5)とともに、減算フラグをONにして(S6)、利用金額の減算を可能にする。

【0014】この処理は、最初のカード出荷時の処理、あるいは全額使用した後の再設定時の処理であり、デ

タエリアの管理者権限を持つ認証の成功が条件であるため、セキュリティを向上させることができ、特にパスワード照合、暗号認証、生体認証を組み合わせることにより、データエリアの属性管理を格段に向上させることができる。

【0015】図3は減算処理フローを示す図である。減算処理は、減額要求待ちの状態にあって、利用額に応じた減額要求があると(S11)、パスワード照合が行われる(S12)。もちろん、パスワード照合に代えて暗号認証等の他の認証方法でもよい。パスワードが一致すれば(S13 YES)、ICカードのデータエリア内の減算フラグを参照していく。パスワードが一致しなければ(S13 NO)処理は終了する。参照した結果、減算フラグがONであれば(S14 YES)、プリペイド領域の減算可能金額(残額)が、減算要求額より大きいのか否か比較判断する(S15)。減算フラグがOFFであれば処理は終了する。残額が減算要求額より大きく減算可能であれば(S15 YES)、減算処理を実行する(S16)。残額が減算要求額より小さく減算不可能であれば(S15 NO)、減算フラグをOFFにし(S17)、フラグがOFFであることを外部へ通知する(S18)。なお、S15において、残額が一定基準額を下回った段階で減算フラグをOFFにして減額を禁止するようにしてもよい。こうして、減算フラグがOFFになると、図2の処理フローにより、再度、購買可能金額の設定、フラグの再設定を行うことにより購買可能となる。

【0016】このように、データエリアごとに設定したフラグにより演算命令を制御しているので、カード外からの不正なアクセスを防止することが可能である。

【0017】

【発明の効果】以上のように本発明によれば、演算命令が演算できないような不適切なエリアに適用されてしまうのを防止することができ、また、演算が実施できるか否かは、対象データ領域ごとに管理されているため、カード外からの不正なアクセスの防止をより効果的に行うことができる。また、カード内部にフラグを設定することで、専用のファイルの種類を増やすことなく、データエリアの属性管理を行うことができる。また、フラグの解除や再設定では、管理者のみがカードとの認証機能を用いることができるため、セキュリティが向上することができる。特にパスワード認証だけでなく、管理者用のICカードとの暗号認証や生体認証などを組み合わせることにより、データエリアの属性管理をより強固にすることができる。

【図面の簡単な説明】

【図1】EEPROMのデータファイルを説明する図である。

【図2】購買可能金額の設定処理フローを説明する図である。

10

20

30

40

50

5

6

【図 3】 減算処理フローを説明する図である。

【図 4】 リーダ/ライタと IC カードの通信を説明する図である。

【図 5】 IC カードの構成を説明する図である。

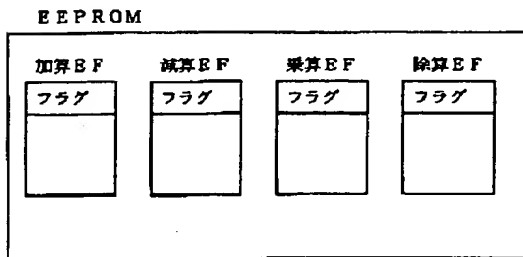
【図 6】 パスワード照合を説明する図である。

【図 7】 パスワード照合を説明する図である。

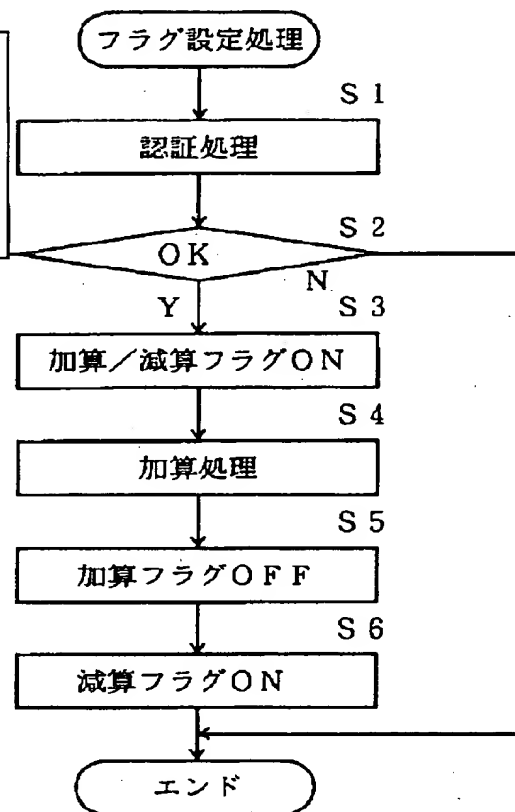
【符号の説明】

1 … リーダ/ライタ、2 … IC カード、2 a … CPU、
2 d … EEPROM

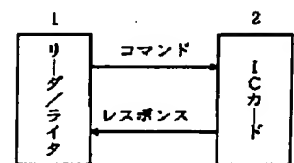
【図 1】



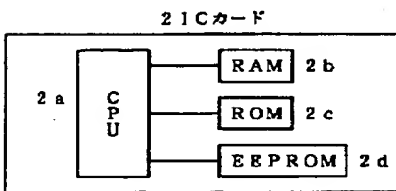
【図 2】



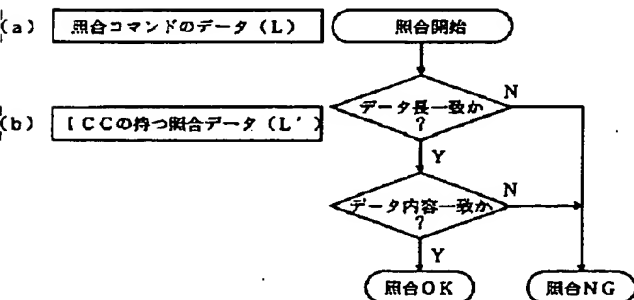
【図 4】



【図 5】



【図 6】



【図 7】

【図 3】

